

Hassan A. Zavareei (SBN 181547)
Katherine M. Aizpuru (*pro hac vice to be filed*)
hzavareei@tzlegal.com
kaizpuru@tzlegal.com
TYCKO & ZAVAREEI LLP
2000 Pennsylvania Avenue, Northwest, Suite 1010
Washington, District of Columbia 20006
Telephone: (202) 973-0900

Attorneys for Plaintiff and the Proposed Class

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA**

WILLIAM MARTIN, on behalf of himself
and all others similarly situated,

Plaintiff,

v.

META PLATFORMS, INC.,

Defendant.

Case No.

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiff William Martin, individually and on behalf of all others similarly situated, by and through counsel, hereby brings this action against defendant Meta Platforms, Inc. Plaintiff's allegations herein are based upon personal knowledge and belief as to their own acts and upon the investigation of their counsel, and information and belief as to all other matters.

NATURE OF THE CASE

“Based on what we’ve seen so far, we consider these to be severe violations of our anti-tracking policies.” – Mozilla, creator of the Firefox browser

1. On June 3, 2025, cybersecurity researchers revealed a novel covert tracking method deployed by Meta Platforms, Inc. (“Defendant” or “Meta”) against potentially billions of Android users.¹ The researchers found that Meta had been using its Instagram and Facebook mobile apps to secretly spy upon users’ mobile web browsing activities. Meta then deanonymized the web browsing information gleaned from this surreptitious monitoring and linked it to users’ identities to craft detailed user profiles, which, in turn, Meta can use for its own profits.

2. According to the researchers, Meta’s furtive and unauthorized tracking “bypasses typical privacy protections such as clearing cookies, Incognito Mode and Android’s permission controls. Worse, it opens the door for potentially malicious apps eavesdropping on users’ web activity.”²

3. Meta’s spying techniques shocked its peers in the tech space with its invasiveness and disregard for consumer expectation and industry-wide privacy norms.³ A representative of Google, which makes Android devices, told tech news outlet Ars Technica that the practice “blatantly violate[s] our security and privacy principles.”⁴ Mozilla told the reporter that “[b]ased on what we’ve seen so far, we consider these to be severe violations of our anti-tracking policies, and are assessing solutions to protect against these new tracking technologies.”⁵ Other web browser developers, including DuckDuckGo and

¹ See Local Mess, Disclosure: Covert Web-to-App Tracking via Localhost on Android, <https://localmess.github.io/> (last accessed by counsel on June 5, 2025).

² *Id.*

³ Dan Goodin, *Meta and Yandex are de-anonymizing Android users’ web browsing identifiers*, Ars Technica (June 3, 2025), <https://arstechnica.com/security/2025/06/meta-and-yandex-are-de-anonymizing-android-users-web-browsing-identifiers/>.

⁴ *Id.*

⁵ *Id.*

1 Brave, are actively trying to mitigate the techniques despite experts' warnings that their ability to do so
2 over the long term could "become ineffective at any time."⁶

3 4. Meta's sneaky spying is just the latest iteration of its well-documented disregard for
4 privacy and security in pursuit of profits. Meta's primary source of revenue is digital advertising,
5 including via amassing vast quantities of data about consumers that it can leverage for advertisers and
6 businesses. When Meta can link information about consumers' browsing activities to their Instagram and
7 Facebook profiles, the opportunity to target them with advertisements will be worth more to advertisers
8 who can benefit from the more detailed profiles. Meta's bottomless appetite for consumer data and the
9 profits that data brings has motivated it to disregard consumer privacy for decades.

10 5. This latest egregious effort to circumvent consumer privacy expectations was undertaken
11 in violation of federal and California privacy law, without user consent.

12 6. Plaintiff is an Android user with a Facebook and Instagram account who, like others, was
13 affected by Meta's tracking practices. Plaintiff now brings this action to enforce his privacy rights and
14 seek damages for the harm Meta caused by the collection, deanonymization, and sale of his personal
15 information.

16 **THE PARTIES**

17 7. Plaintiff William Martin is a citizen and resident of California.

18 8. Defendant Meta Platforms, Inc. is a Delaware corporation with its principal place of
19 business at 1 Meta Way, Menlo Park, CA 94025.

20 **JURISDICTION AND VENUE**

21 9. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act, 28
22 U.S.C. § 1332(d). The aggregated claims of the individual class members exceed the sum or value of
23 \$5,000,000.00, exclusive of interest and costs; there are more than 100 putative class members; and at
24 least one putative class member is from a state different from the Defendant.

25 10. This Court has personal jurisdiction over Defendant because it maintains a principal place
26 of business in this District.

27
28

⁶ *Id.*

11. Venue is proper in this judicial district under 28 U.S.C § 1391 because Defendant resides in this District.

FACTS COMMON TO THE CLASS

A. Meta’s operates a profitable advertising business based on amassing user information for targeted ads.

12. Meta’s Facebook platform is among the most popular social media platforms in the world. Facebook has roughly 3 billion monthly average users and 2.11 billion daily users. Over half of the world’s active internet users access Facebook every month.⁷

13. Instagram is also hugely popular, boasting 171.7 million users in the United States alone and 2 billion monthly active users.⁸

14. The vast majority of Meta’s revenue comes from advertising. In the first quarter of 2025, Meta earned over \$41 billion in revenue from advertising—97% of its quarterly revenue.

15. Meta’s advertising capabilities are linked to its ability to track consumers’ activity across millions of websites and advertisements—regardless of whether particular consumers use its platforms.⁹ Meta’s tracking capabilities allow it to target users with advertisements tailored to the information it has gathered about them, including through the Meta Pixel. Specifically, Meta compiles the information it collects into a dataset called “Core Audiences” and “Custom Audiences” that advertisers can use to target marketing efforts. When Apple implemented privacy measures to impede Meta’s ability to track user data, Meta lost *billions* of dollars in revenue as a result.¹⁰

16. Meta’s tracking pixel (the Meta Pixel) is one of the tools that Meta uses to collect information about consumers for its advertising business. The Meta Pixel is a piece of tracking code that

⁷ Facebook User & Growth Statistics, BLACKLINKO, <https://backlinko.com/facebook-users> (last updated Jan. 30, 2025)

⁸ See Instagram – statistics & facts, STATISTA, <https://www.statista.com/topics/1882/instagram> (last visited by counsel June 5, 2025).

⁹ See Lena Cohen, *Mad at Meta? Don’t Let Them Collect and Monetize Your Personal Data*, Electronic Frontier Foundation (Jan. 17, 2025), <https://www.eff.org/deeplinks/2025/01/mad-meta-dont-let-them-collect-and-monetize-your-personal-data>.

¹⁰ Kate O’Flaherty, *Apple’s Stunning \$10 Billion Blow to Facebook*, Forbes (Nov. 6, 2021), <https://www.forbes.com/sites/kateoflahertyuk/2021/11/06/apples-new-iphone-privacy-features-cost-facebook-10-billion/>.

web developers can install on their websites to “measure, optimize and build audiences for . . . ad campaigns.”¹¹ The Meta Pixel is found on 30% of the world’s most popular websites. It monitors consumers’ behavior and can expose sensitive information, including financial and health data. In addition to its own users, Meta also tracks non-users across the web through the Meta Pixel.

17. The Meta Pixel logs when someone takes action on a website (an “event”) such as adding items to a cart, making a purchase, inputting information into a form, or visiting pages. Meta offers a menu of “standard events” so that advertisers can choose what information they want the Meta Pixel to track when it has been embedded on a website, and even allows advertisers to create their own “custom events” separate from the tracking information that Meta offers standard. Meta offers step-by-step instructions for installing the Meta Pixel so that companies can add it to their website without a developer.

18. By design, the Meta Pixel is invisible to consumers.

19. When a user visits a website on which the Meta Pixel has been installed, Meta’s software surreptitiously directs the user’s browser to separately send a message to Meta’s servers containing the user’s communications with the website—the data that the Meta Pixel is configured to collect, such as pages browsed, items placed into a cart or purchased, and information entered into forms, among other things. In 2022, an investigation found that a third of the top U.S. hospitals had sent sensitive patient information to Meta through the Meta Pixel.¹² After intercepting and collecting this data, Meta analyzes it and includes it in its datasets.

20. Meta does not require websites that install the Meta Pixel to have obtained user consent to have their private information transmitted to Meta.

B. Mobile devices come standard with privacy controls that inhibit certain tracking and deanonymization because consumers don’t want to be spied on.

21. Meta is well aware that consumers do not want to be spied on while using the internet. Meta has been sued repeatedly for using the Meta Pixel to surreptitiously monitor users’ internet activity

¹¹ Meta, Meta Pixel (2025), <https://www.facebook.com/business/tools/meta-pixel>.

¹² See Cohen, *supra* note 9.

1 for Meta’s own profit. And Meta has been rightly criticized by industry experts for eroding consumers’
2 ability to control their own information.¹³

3 22. Because of this, many consumer tech companies design their products to allow users the
4 ability to control the extent to which they are tracked. And privacy norms have arisen in the tech space
5 that facilitate consumer control over information and privacy.

6 23. For example, as one researcher explained, “[o]ne of the fundamental security principles
7 that exists in the web, as well as the mobile system, is called sandboxing.”¹⁴ Sandboxing is a technique
8 that isolates mobile apps from one another, including from web browsers, to protect each app and the
9 system as a whole from malicious applications.¹⁵ By default, apps can’t interact with each other and have
10 limited access to the operating system. As Google explains to its users on its Android development site,
11 “[i]f app A tries to do something malicious, such as read app B’s data or dial the phone without
12 permission, it’s prevented from doing so The sandbox is simple, auditable, and based on decades-
13 old . . . separation of processes and file permissions.”¹⁶

14 24. Partitioning is another method of allowing users to maintain control over their data.
15 Mozilla, the creator of the Firefox browser, uses “state partitioning” to “mitigate the ability of websites”
16 to engage in cross-site tracking.¹⁷ This technical process does not prevent technologies like cookies from
17 tracking consumer behavior on websites, but it does prevent an ad tracking technology from storing an
18 identifier that can be retrieved from multiple websites and used to identify a user’s online behavior.¹⁸
19 Similarly, Google Chrome uses “storage partitioning” to “prevent certain types of side-channel cross-site
20 tracking.”¹⁹

22 ¹³ See Kurt Opsahl, *Facebook’s Eroding Privacy Policy: A Timeline*, Electronic Frontier Foundation (Apr.
23 28, 2010), <https://www.eff.org/deeplinks/2010/04/facebook-timeline>.

24 ¹⁴ Goodin, *supra* note 3.

25 ¹⁵ See Application Sandbox, Android, <https://source.android.com/docs/security/app-sandbox> (last visited
26 by counsel June 5, 2025).

27 ¹⁶ *Id.*

28 ¹⁷ See State Partitioning, Mozilla, [https://developer.mozilla.org/en-
US/docs/Web/Privacy/Guides/State_Partitioning](https://developer.mozilla.org/en-US/docs/Web/Privacy/Guides/State_Partitioning) (last visited by counsel June 5, 2025).

¹⁸ *Id.*

¹⁹ See Storage Partitioning, Google Privacy Sandbox, <https://privacysandbox.google.com/cookies/storage-partitioning> (last visited by counsel June 5, 2025).

25. Defenses such as state partitioning and storage partitioning are built into all major browsers and are intended to ensure that site cookies for one website are off limits for others.²⁰

C. Meta deployed abusive and surreptitious new tracking techniques that wrongfully override industry norms and consumer expectations.

26. As of at least September 2024 through June 3, 2025, Meta, in its insatiable thirst for consumer information, developed and deployed a new tracking technique that overrode and evaded these important privacy norms and policies to allow Meta to secretly track and deanonymize user information.

27. Meta’s new technology allowed Meta to bypass protections in browsers like Chrome and Firefox and pass cookies and other identifiers from websites to native Android apps for Facebook and Instagram. Meta could then “tie that vast browsing history to the account holder logged into the app.”²¹

28. Indeed, it was not enough that the Meta Pixel was already gathering user information and sending it directly to Meta. Instead, Meta developed a *new* technique to flawlessly *link* information obtained through the Meta Pixel and send it to Meta deanonymized. As the researchers who discovered this scheme explained, “this method effectively allows [Meta] to link mobile browsing sessions and web cookies to user identities, hence de-anonymizing users’ visiting sites embedding their scripts.”²²

29. This is how it works²³:

- a. First, the user opens the native Facebook or Instagram app, which is eventually sent to the background. The app creates a background service to listen for incoming traffic on a TCP port and a UDP port. The user must be logged in, but these app keep users logged in perpetually.
- b. Then, the user opens their browser, such as Chrome or Firefox, and visits a website embedded with the Meta Pixel. Again, approximately 30% of the world’s most popular website have the Meta Pixel installed. At this stage, the website *may* (but does not always) ask for user consent depending on the website’s and visitor’s locations.

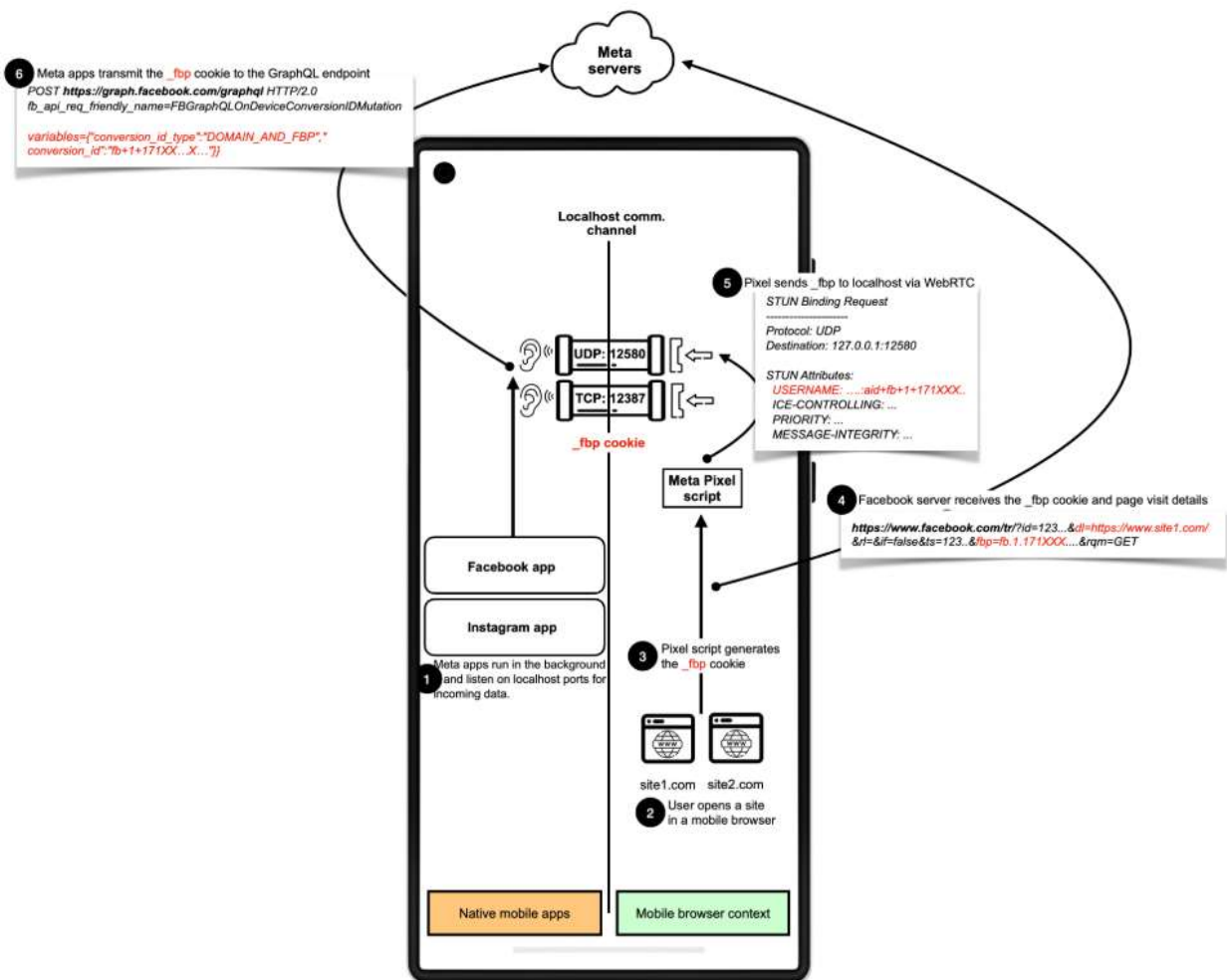
²⁰ See Goodin, *supra* note 3.

²¹ *Id.*

²² See Local Mess, *supra* note 1.

²³ *Id.*

- c. The Meta Pixel script then sends the `_fbp` cookie (which, according to Meta, “identifies browsers for the purposes of providing advertising and site analytics services”) to the native Facebook or Instagram app, and also sends the `_fbp` value (which includes information like page URL, metadata, and the event type, such as PageView, AddtoCart, Purchase, etc.) to Meta.
- d. Finally, the Facebook and Instagram apps receive the `_fbp` cookie from the Meta Pixel script running on the browser. The apps then link the information conveyed to other persistent user identifiers, linking the users’ visits with their Facebook or Instagram account.



30. As reported by ArsTechnica, this technique abuses basic functionality built into modern mobile browsers. It allows the Meta Pixel to escape the “sandbox” and link browsing activity on the

mobile browser with identifying information on the Facebook and Instagram apps. In this way it renders the browsing history of Android users completely identifiable.

31. This technique operates without user consent. Meta did not seek or obtain user consent to link their browsing activity with their Instagram and Facebook app identifiers in this manner.

32. This new web-to-app ID sharing method “bypasses typical privacy protections such as clearing cookies, Incognito Mode, and Android’s permission controls. Worse, it opens the door for potentially malicious apps eavesdropping on users’ web activity.”²⁴

D. Meta did not disclose these surreptitious new techniques.

33. Meta did not disclose its surreptitious new techniques. Indeed, even websites with Meta Pixels installed were not aware of and did not consent to Meta’s new techniques.²⁵ And Meta’s peers in the tech space were shocked by these revelations. A representative for Google told ArsTechnica that the conduct violated its terms of service, and Mozilla called it a “blatant violation” of its privacy policies.²⁶

34. Meta’s Privacy Policy did not disclose these new techniques either.

35. Accordingly, Meta did not and could not have obtained consumer consent for its practices.

E. Meta has a history of flouting consumer privacy.

36. Since at least 2012, Meta has been required to police its own privacy violations. On July 27, 2012, the Federal Trade Commission entered an order pursuant to a consent agreement with Meta wherein Meta was ordered not to misrepresent “the extent to which it maintains the privacy or security of covered information,” including its collection or disclosure of the information, consumer control over covered information, and steps it takes to verify third party security. Covered information includes “information from or about an individual consumer, including name, address, email address, phone number, IP address, User ID or other persistent identifier, physical location, or any information combined with any of the above.” Meta also agreed to maintain a “comprehensive privacy program.” On April 27, 2020, the FTC modified the 2012 order and issued a new consent order adding additional provisions.

²⁴ *Id.*

²⁵ *See id.*

²⁶ *See Goodin, supra* note 3

PLAINTIFF'S FACTUAL ALLEGATIONS

37. Plaintiff owns and uses a Samsung 21 Ultra 56 phone that runs on the Android operating system.

38. Plaintiff has an Instagram account and a Facebook account. Between September 2024 and June 3, 2025, Plaintiff has had the Facebook app and Instagram app installed on Plaintiff's Android mobile phone. He was logged in to those accounts on his phone.

39. Between September 2024 and June 3, 2025, while the Facebook and Instagram apps were installed, logged in, and running on Plaintiff's Android-based mobile phone, Plaintiff visited websites where the Meta Pixel was installed.

40. Unbeknownst to Plaintiff and without Plaintiff's consent, when Plaintiff visited those websites, everything Plaintiff did on those websites was collected in Meta by the Meta Pixel. And unbeknownst to Plaintiff and without Plaintiff's consent, Meta used the tracking tools described above to tie Plaintiff's website behavior to his Facebook and Instagram profiles, thus de-anonymizing and identifying Plaintiff and Plaintiff's browsing information in real time.

41. Meta compiled this information to create a comprehensive profile of Plaintiff in its databases for uses in advertising. Plaintiff's data became more valuable to Meta based on its identifiability which was only available to Meta through its wrongful and surreptitious acts.

CHOICE OF LAW ALLEGATIONS

42. Because this Complaint is brought in California, California's choice of law regime governs the state law allegations in this Complaint. Under California's governmental interest/comparative impairment choice of law rules, California law applies to the claims of all Class members, regardless of their state of residence or state of purchase.

43. Further, under Meta's Terms of Service, California law applies to claims arising from Plaintiff's use of Meta.

CLASS ACTION ALLEGATIONS

44. Plaintiff brings this suit as a class action on behalf of themselves and on behalf of all others similarly situated pursuant to Federal Rule of Civil Procedure 23. This action satisfies the numerosity,

commonality, typicality, adequacy, predominance and superiority requirements of the provisions of Rule 23.

45. Plaintiff seeks to represent the following Nationwide Class: **Android users in the United States with a Facebook or Instagram account who (1) have the Facebook or Instagram app installed on their Android phone, (2) used their Android phone to visit a website with the Meta Pixel installed between September 2024 and June 3, 2025, (3) while logged into their Facebook or Instagram account, and (4) had their browsing information collected by Meta.**

46. The Nationwide Class will be referred to collectively as the “Class.” Excluded from the Class are Defendant, any affiliate, parent, or subsidiary of Defendant, any entity in which Defendant has a controlling interest, any officer or director of Defendant, and any judge to whom this case is assigned.

47. ***Numerosity:*** Members of the Class(es) are so numerous that joinder of all members is impracticable. It is estimated that there are tens or hundreds of millions of individuals in the Class. The identity of such membership is readily ascertainable from Defendant’s records and non-party records.

48. ***Commonality:*** This action involves common questions of law and fact, which predominate over any questions affecting individual Class Members. These common legal and factual questions include, but are not limited to, the following:

- a. Whether Defendant’s conduct was an egregious breach of social norms;
- b. Whether Defendant acted intentionally;
- c. Whether Defendant was unjustly enriched; and
- d. Whether Plaintiff and the Class Members are entitled to damages, the measure of damages, statutory damages, or other relief.

49. ***Typicality:*** Plaintiff’s claims are typical of those of the other Class Members because, *inter alia*, all members of the Class(es) were injured through the common misconduct described above. Plaintiff is advancing the same claims and legal theories on behalf of themselves and all members of the Class(es).

50. ***Adequacy of Representation:*** Plaintiff will fairly and adequately represent and protect the interests of the Class in that they have no disabling conflicts of interest that would be antagonistic to those of the other Class Members. Plaintiff seeks no relief that is antagonistic or adverse to the other

1 Class Members and the infringement of the rights and the damages they have suffered are typical of other
2 Class Members. Plaintiff has retained counsel experienced in complex consumer class action litigation,
3 and intends to prosecute this action vigorously.

4 51. ***Superiority:*** Class litigation is an appropriate method for fair and efficient adjudication of
5 the claims involved. Class action treatment is superior to all other available methods for the fair and
6 efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members
7 to prosecute their common claims in a single forum simultaneously, efficiently, and without the
8 unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would
9 require. Class action treatment will permit the adjudication of relatively modest claims by certain Class
10 Members, who could not individually afford to litigate a complex claim against large corporate
11 defendants. Further, even for those Class Members who could afford to litigate such a claim, it would
12 still be economically impractical.

13 52. The nature of this action and the nature of laws available to Plaintiff and the Class make
14 the use of the class action device a particularly efficient and appropriate procedure to afford relief to
15 Plaintiff and the Class Members for the wrongs alleged because Defendant would necessarily gain an
16 unconscionable advantage since they would be able to exploit and overwhelm the limited resources of
17 each individual Class Member with superior financial and legal resources. The costs of individual suits
18 could unreasonably consume the amounts that would be recovered. Further, proof of a common course
19 of conduct to which Plaintiff were exposed is representative of that experienced by the Class and will
20 establish the right of each member of the Class to recover on the cause of action alleged, and individual
21 actions would create a risk of inconsistent results and would be unnecessary and duplicative of this
22 litigation.

23 53. Plaintiff reserves the right to modify or amend the definition of the proposed Class and
24 (alternative) state classes before the Court determines whether certification is appropriate and as the
25 parties engage in discovery.

26 54. The class action is superior to all other available methods for the fair and efficient
27 adjudication of this controversy. Because of the number and nature of common questions of fact and law,
28 multiple separate lawsuits would not serve the interest of judicial economy.

55. Individual litigation of the claims of all Class Members is economically unfeasible and procedurally impracticable. While the aggregate damages sustained by the Class Members are likely in the millions of dollars, the individual damages incurred by each Class Member resulting from Defendant's wrongful conduct are too small to warrant the expense of individual suits. The likelihood of individual Class Members prosecuting separate claims is remote, and even if every Class Member could afford individual litigation, the court system would be unduly burdened by individual litigation of such cases. Individual Class Members do not have a significant interest in individually controlling the prosecution of separate actions, and the individualized litigation would also present the potential for varying, inconsistent, or contradictory judgments and would magnify the delay and expense to all parties and to the court system resulting from multiple trials of the same factual issues. Plaintiff knows of no difficulty to be encountered in the management of this action that would preclude its maintenance as a class action. A class action in this matter will avoid case management difficulties and provide multiple benefits, including efficiency, economy of scale, unitary adjudication with consistent results and equal protection of the rights of each Class member, all by way of the comprehensive and efficient supervision of the litigation by a single court.

56. Notice of a certified class action and of any result or resolution of the litigation can be provided to Class Members by first-class mail, email, or publication, or such other methods of notice as deemed appropriate by the Court.

57. Plaintiff does not anticipate any difficulty in the management of this litigation.

FIRST CLAIM FOR RELIEF
INTRUSION UPON SECLUSION UNDER CALIFORNIA LAW
(By Plaintiff on Behalf of the Nationwide Class)

58. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

59. To state a claim for intrusion upon seclusion, Plaintiff must possess a legally protected privacy interest and a reasonable expectation of privacy. Further, Plaintiff must show that the intrusion is so serious in nature, scope, and actual or potential impact as to constitute an egregious breach of social norms.

1 60. Plaintiff and the Class Members have an interest in maintaining control over their web
2 browsing activity, preventing the dissemination of that activity to third parties without consent, and
3 making decisions about internet use without observation, intrusion, or interference. Plaintiff and the Class
4 Members have the right to use the internet without Meta observing their use of websites in a way that
5 identifies them to Meta.

6 61. Plaintiff and the Class Members also had a reasonable expectation that their
7 communications with websites, identities, personal activities, and other data would remain confidential
8 and that Meta would not use secret technologies to deanonymize that information and use it for targeted
9 advertising without having obtained their express, informed consent. Plaintiff and the Class Members did
10 not authorize Meta to intercept data on every aspect of their internet use and link it to their identifying
11 information.

12 62. By overriding ordinary standard privacy and security controls to link mobile browsing
13 activity with identifying information in the Instagram and Facebook apps, Defendant invaded Plaintiff
14 and the Class Member's privacy rights and intruded upon their seclusion.

15 63. The conduct complained of herein is highly offensive to a reasonable person and is an
16 egregious breach of social norms, including in that (1) Meta abused its communication channels in
17 violation of browsers' privacy policies, and (2) Meta undertook to collect this information surreptitiously
18 because Meta knew that consumers would not agree to it. Meta's conduct overrode privacy controls such
19 as Incognito Mode and cookie deletion, allowing Meta to evade protocols to prevent exactly what it was
20 doing. Meta placed profits over privacy.

21 64. Defendant was enriched through these practices because its profiles of consumers became
22 more valuable when Meta exploited Android communication channels to tie browsing information to
23 user identities.

24 65. Plaintiff and the Class Members seek all relief available for these invasions of privacy.
25
26
27
28

SECOND CLAIM FOR RELIEF
VIOLATION OF THE CALIFORNIA INVASION OF PRIVACY ACT (Wiretapping)
Cal. Penal Code § 631
(By Plaintiff on Behalf of the Nationwide Class)

66. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

67. California Penal Code Section 630 recognizes that “advances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society.”

68. At all relevant times, there was in full force and effect the California Wiretapping Act, Cal. Penal Code § 631.

69. The California Wiretapping Act provides that:
any person . . . who willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or who aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section[.]

70. Meta is a person within the meaning of the California Wiretapping Act. Meta was within the state of California at all relevant times herein.

71. The data and transmissions between Plaintiff and the Class Members, on the one hand, and the websites they visited on their mobile browsers, on the other, are messages, reports, and/or communications within the scope of the California Wiretapping Act as they are transfers of signals, data, and intelligence transmitted by a wire, line, or cable system.

72. As described herein, Meta intercepted in real time and as they were transmitted the contents of these communications and have diverted these communications to itself without consent.

73. Meta then deanonymized the communications and tied them to the identities of individual Facebook and Instagram users.

1 74. The Instagram and Facebook apps constitute a machine, instrument or contrivance that
2 taps or makes unauthorized connections by listening to traffic on a TCP and UDP port, thereby
3 monitoring website use.

4 75. Plaintiff and the Class Members have a reasonable expectation of privacy in their web
5 browsing on their own mobile devices.

6 76. Meta intentionally used or endeavored to use the contents of the intercepted
7 communications knowing or having reason to know that it was obtained through unlawful interception.

8 77. Meta has disclosed and used the contents of the intercepted communications by selling
9 Plaintiff's and the Class Members' information to third parties for financial and commercial benefit,
10 obtaining substantial profits.

11 78. Meta knew or should have known that the intercepted communications were captured in
12 secret and in violation of the Act because the conduct violated Google's privacy policy, Mozilla's privacy
13 policy, and user expectations; its conduct was designed to and did override privacy controls like Incognito
14 Mode and cookie clearing; Meta did not publicize its techniques and instead kept them secret; and the
15 nature of the communications were such that they had to be obtained via wiretap.

16 79. Plaintiff and the Class Members were not aware of Meta's conduct and could not have
17 and did not consent to the collection and deanonymization of their data this way.

18 80. As a direct and proximate result of Defendants' violations of the California Wiretapping
19 Act, Plaintiff and the Class Members were injured and suffered damages, a loss of privacy, and loss of
20 the value of their personal information in an amount to be determined at trial.

21 81. Defendant was unjustly enriched by its violations of the California Wiretapping Act.

22 82. Pursuant to California Penal Code Section 637.2, Plaintiff and the Class Members have
23 been injured by Defendants' violations, and seek damages for the greater of \$5,000 or three times the
24 amount of actual damages, and injunctive relief, plus reasonable attorneys' fees and costs.

THIRD CLAIM FOR RELIEF
VIOLATIONS OF THE CALIFORNIA INVASION OF PRIVACY ACT
Cal. Penal Code § 635
(By Plaintiff on Behalf of the Nationwide Class)

83. Plaintiff incorporate by reference all allegations of the preceding paragraphs as though fully set forth herein.

84. At all relevant times, there was in full force and effect California Penal Code § 635, which provides that “every person who manufactures, assembles, sells, offers for sale, advertises for sale, possesses, transports, imports, or furnishes to another any device which is primarily or exclusively designed or intended for eavesdropping upon the communication of another” shall be guilty of a crime.

85. The novel code that Meta used to tie users’ communications with websites to their identities are “devices” “primarily or exclusively designed or intended for eavesdropping upon the communication of another.” Meta manufactured, assembled, sold, offered, advertised, possessed, and furnished these devices.

86. Plaintiff and the Class Members were not aware of Meta’s conduct and could not have and did not consent to the collection and deanonymization of their data this way.

87. As a direct and proximate result of Defendants’ violations of the Cal. Penal Code § 635, Plaintiff and the Class Members were injured and suffered damages, a loss of privacy, and loss of the value of their personal information in an amount to be determined at trial.

88. Defendant was unjustly enriched by its violations.

89. Pursuant to California Penal Code Section 637.2, Plaintiff and the Class Members have been injured by Defendants’ violations, and seek damages for the greater of \$5,000 or three times the amount of actual damages, and injunctive relief, plus reasonable attorneys’ fees and costs.

FOURTH CLAIM FOR RELIEF
VIOLATIONS OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT
18 U.S.C. §§ 2511(1), *et seq.*
(By Plaintiff on Behalf of the Nationwide Class)

90. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

1 91. The Electronic Communications Privacy Act (“ECPA”) makes it illegal intentionally to
2 intercept, or attempt to intercept, any wire, oral, or electronic communication and to disclose or use the
3 contents of an unlawfully intercepted communication. 18 U.S.C. § 2511.

4 92. ECPA provides a private right of action to any person whose electronic communications
5 are intercepted. 18 U.S.C. § 2520(a).

6 93. Defendant intentionally intercepted electronic communications that Plaintiff and the Class
7 Members exchanged with third party websites when it captured them using the Meta Pixel and used its
8 novel technologies to deanonymize them.

9 94. The transmission of data between Plaintiff and the Class Members and third party websites
10 qualifies as communications under ECPA. 18 U.S.C. § 2510(12).

11 95. Defendant contemporaneously intercepted and transmitted Plaintiff’s and the Class
12 Members’ communications of that data. Meta was not a party to those communications.

13 96. The Meta Pixel and the code that Defendant used to deanonymize the browsing activity
14 are all “devices” within the meaning of 18 U.S.C. § 2510(5).

15 97. Plaintiff and the Class members did not consent to Meta’s acquisition of these
16 transmissions or its deanonymization of the same.

17 98. By using the contents of Plaintiff’s and the Class Members’ electronic communications,
18 while knowing the information was obtained through interception of an electronic communication in
19 violation of 18 U.S.C. § 2511(1)(a), Meta violated 18 U.S.C. § 2511(1)(d)..

20 99. Plaintiff and the Class members have suffered damages because of Defendant’s violations
21 of ECPA.

22 100. Plaintiff and the Class members seek appropriate declaratory or equitable relief including
23 injunctive relief, actual damages and profits enjoyed by Defendant as a result of violations or the
24 appropriate statutory measure of damages, punitive damages, and reasonable attorneys’ fees and costs.
25 18 U.S.C. § 2520. Pursuant to 18 U.S.C. § 2520, Plaintiff and the Class Members seek monetary damages
26 for the greater of (i) the sum of the actual damages suffered by the plaintiff and any profits made by
27 Defendant as a result of the violation or (ii) statutory damages of whichever is greater of \$100 a day for
28 each violation or \$10,000.

FIFTH CLAIM FOR RELIEF
UNJUST ENRICHMENT
(By Plaintiff on Behalf of the Nationwide Class)

101. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

102. Plaintiff and the Class Members conferred a benefit on Defendant by utilizing Instagram and Facebook accounts which Defendant then utilized, without Plaintiff's or the Class Members' consent, to eavesdrop on their web browsing activity and deanonymize it. Defendant used that wrongfully gotten information for its advertising business and profits.

103. Defendant had knowledge that this benefit was conferred upon it.

104. Defendant retained that benefit under circumstances that make it unjust and inequitable for Defendant to retain it without paying Plaintiff and Class Members the value thereof.

105. Defendant has been unjustly enriched at the expense of Plaintiff and the Class and its retention of this benefit under the circumstances would be inequitable.

106. Plaintiff seeks an order requiring Defendant to make restitution to them and the other members of the Class.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of themselves and all others similarly situated, respectfully request that this Court:

a. Determine that the claims alleged herein may be maintained as a class action under Federal Rule of Civil Procedure 23, and issue an order certifying the Class;

b. Appoint Plaintiff as representatives of the Class;

c. Appoint Plaintiff's counsel whose appearance is noticed herein as Class Counsel;

d. Award all actual, general, special, incidental, statutory, punitive, exemplary, and consequential damages and restitution to which Plaintiff and Class Members are entitled in an amount to be determined at trial and require Meta to disgorge its ill-gotten gains;

e. Award pre-judgment and post-judgment interest on such monetary relief at the highest legal rate to the extent provided by law;

f. Grant appropriate injunctive and/or declaratory relief;

- 1 g. Award reasonable attorneys' fees and costs to the extent provided by law; and
2 h. Grant such further relief that this Court deems appropriate.

3
4 **JURY DEMAND**

5 Plaintiff demands a trial by jury on all issues so triable.

6 DATED: June 6, 2025

By: /s/ Hassan A. Zavareei

7 Hassan A. Zavareei (SBN 181547)

8 Katherine M. Aizpuru*

9 *kaizpuru@tzlegal.com*

TYCKO & ZAVAREEI LLP

10 2000 Pennsylvania Ave NW, Suite 1010

11 Washington, DC 20006

12 Telephone: (202) 973-0900

13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
**pro hac vice to be filed*